PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 — A1

(11) International Publication Number: **WO 99/35553**

(43) International Publication Date: 15 July 1999 (15.07.99)

(21) International Application Number: PCT/GB99/00079

(22) International Filing Date: 11 January 1999 (11.01.99)

(30) Priority Data:
9800443.5 10 January 1998 (10.01.98) GB

(71) Applicant *(for all designated States except US)*: NCIPHER CORPORATION LIMITED [GB/GB]; Jupiter House, Station Road, Cambridge CB1 2JD (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: VAN SOMEREN, Nicholas, Benedict [GB/GB]; 24 Hooper Street, Cambridge CB1 2NZ (GB).

(74) Agent: JONES, Keith, William; Lewis & Taylor, 144 New Walk, Leicester LE1 7JA (GB).

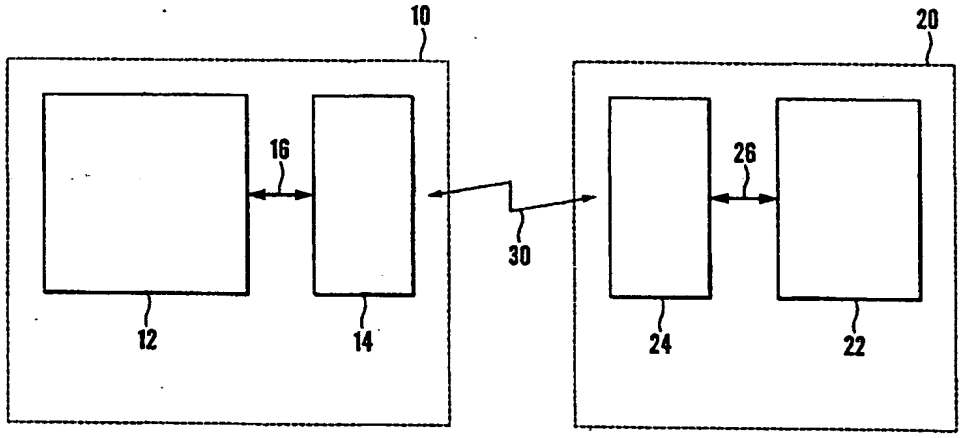
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CRYPTOGRAPHIC TOKEN



(57) Abstract

A data encryption/decryption device (20) for a host computer (10) has an encryption/decryption module (22) which is hard wired with an infrared interface (24) capable of communicating with an infrared interface (14) at the host computer (10). The device (20) is for encrypting/decrypting data received from the computer (10) and transmitting it back to the computer (10), all via the infrared wireless communication link. The device (20) is in the form of a "credit card" sized token.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Cryptographic Token

The present invention relates to cryptographic tokens, and particularly to cryptographic tokens used in conjunction with computer systems.

A cryptographic token is a device which is operative to carry out a cryptographic operation using secret data embedded in the token. Such a device can be used for authentication, the provision of a digital signature, or general encryption and decryption operations. It can be useful in financial and commercial transactions, which increasingly are controlled by computer, requiring some form of reliable authentication of the user to ensure that transactions are properly authorised.

In known systems, cryptographic tokens are used in conjunction with a host computer which has its own cryptographic capability and which is able to carry out some form of interpretation of the information provided by the token.

Cryptographic tokens may have to be placed in a slot in a host computer. On entry into the slot, conductive pads on the card engage with complementary contacts in the slot, so as to provide a direct physical contact. Although such an arrangement is technically satisfactory, it requires the user to perform the steps of inserting the card into the slot, waiting for processing of the card to cease, and removing the card from the slot. A user may wish to perform a number of operations using the token and, for convenience, may leave the token inside the slot until all of the operations are completed. At the end of use of the system, the user may forget to remove the token from the slot, rendering the system open to unauthorised use by a third party. Furthermore, the added steps involved in such a procedure may lead to the procedure being considered too inconvenient for efficient operation of the host system. That may lead to the operator of the host system ignoring the use of the token.

According to the first aspect of the invention, there is provided a data encryption/decryption

device for a host computer comprising encryption/decryption means for performing encryption/decryption operations on data to be used by the host computer and communication means for wireless communications with the host computer, wherein data from the host computer for encryption/decryption is received via the communication means and encrypted/decrypted by the encryption/decryption means, and the encrypted/decrypted data is transmitted back to the host computer via the communication means.

The device according to the invention is particularly advantageous, in that it provides a host system with external cryptographic processing, that is to say, the host system does not need or may not have its own cryptographic capability. Thus, any host system, such as a standard PC, so long as it is capable of establishing a communications link with the device, can take advantage of its cryptographic processing. For example, the host system can rely upon the device for encryption of data which it wishes to send securely through an insecure network or it can rely on the device to decrypt encrypted data which it has received through a network. In either case, no further interpretation of the data needs to be carried out by the host system. What is more, all the cryptographic processing is done within the device, which is where the cryptographic information or keys are stored. Using the keys where they are stored is of benefit because having to move the keys around with the data, as in the case of prior art systems, means increased opportunity for interception and deciphering.

By use of the device according to the invention, no physical connection is necessary, and so no slot need be provided in the host computer. Accordingly, the user of the system in accordance with the invention is less likely to leave the system unattended in an insecure state.

Further aspects and advantages of the invention will now be described, with reference to the drawing in which:

Figure 1 is a schematic view of a cryptographic security system in accordance with a preferred and specific embodiment of the invention.

A host computer 10, such as an IBM compatible personal computer with no cryptographic capability has a central processor 12 and is provided with an integrated infra-red interface 14, adapted to establish an infra-red communications link with an external device.

The interface 14 is hard-wired 16 with the central processor 12, and can be implemented physically by a card inserted into one of the bays commonly provided inside a personal computer for cards such as modems, graphics cards or the like, or encapsulated in a package the same dimensions as a standard disk drive, for insertion in a bay provided for additional disk drives in the host computer 10. Alternatively, the interface can be implemented directly on the motherboard normally provided in a personal computer. Preferably, the package in which the interface 14 is provided is tamper evident and/or access resistant.

A personal security token 20 comprises an encryption/decryption module 22, which in use is operative to perform one or more encryption/decryption operations, and an integrated infra-red interface 24 compatible with the interface 14 of the host computer 10. The interface 24 is hard-wired 26 with the encryption/decryption module 22. The interfaces 14, 24 are operative to establish a wireless communications link 30 between the host computer 10 and the personal security token 20. The encryption/decryption module 22 is operative to encrypt un-encrypted data received from the host computer 10 on the wireless communications link or to decrypt encrypted data received from the host computer 10. In either instance, the encryption/decryption is performed using at least one key stored within the encryption/decryption module 22. After having been processed by the encryption/decryption module 22, the encrypted/decrypted data is transmitted to the host computer 10 on the wireless communication link 30, and the data is used by the host computer 10, for example, for onward transmission to another host or to update/modify software stored in the host computer.

The encryption/decryption operations performed by the encryption/decryption module 22 are preferably performed in conjunction with software or hardware embedded in the host computer 10.

Preferably, the personal security token 20 is in the form of a "credit card" size piece of plastics material, but it may also be embodied on a badge, pendant or a signet-type ring. It may be attached to the person with a flexible member such as a lanyard.

Claims

1. A data encryption/decryption device for a host computer comprising encryption/decryption means for performing encryption/decryption operations on data to be used by the host computer and communications means for wireless communication with the host computer, wherein data from the host computer for encryption/decryption is received via the communication means and encrypted/decrypted by the encryption/decryption means, and the encrypted/decrypted data is transmitted back to the host computer via the communication means.

2. A device according to claim 1 wherein the host computer has no cryptographic capability.

3. A device according to claim 1 or claim 2 wherein at least one key for the encryption/decryption of data is stored within the encryption/decryption means.

4. A device according to any of claims 1 to 3 wherein the communication means comprises an infra-red interface capable of communicating with an infra-red interface at the host computer.

5. A device according to any of claims 1 to 4 which comprises a piece of plastics material, a badge, a pendant or a signet-type ring.

6. A device according to claim 5 which is attached to a user by means of a flexible member.

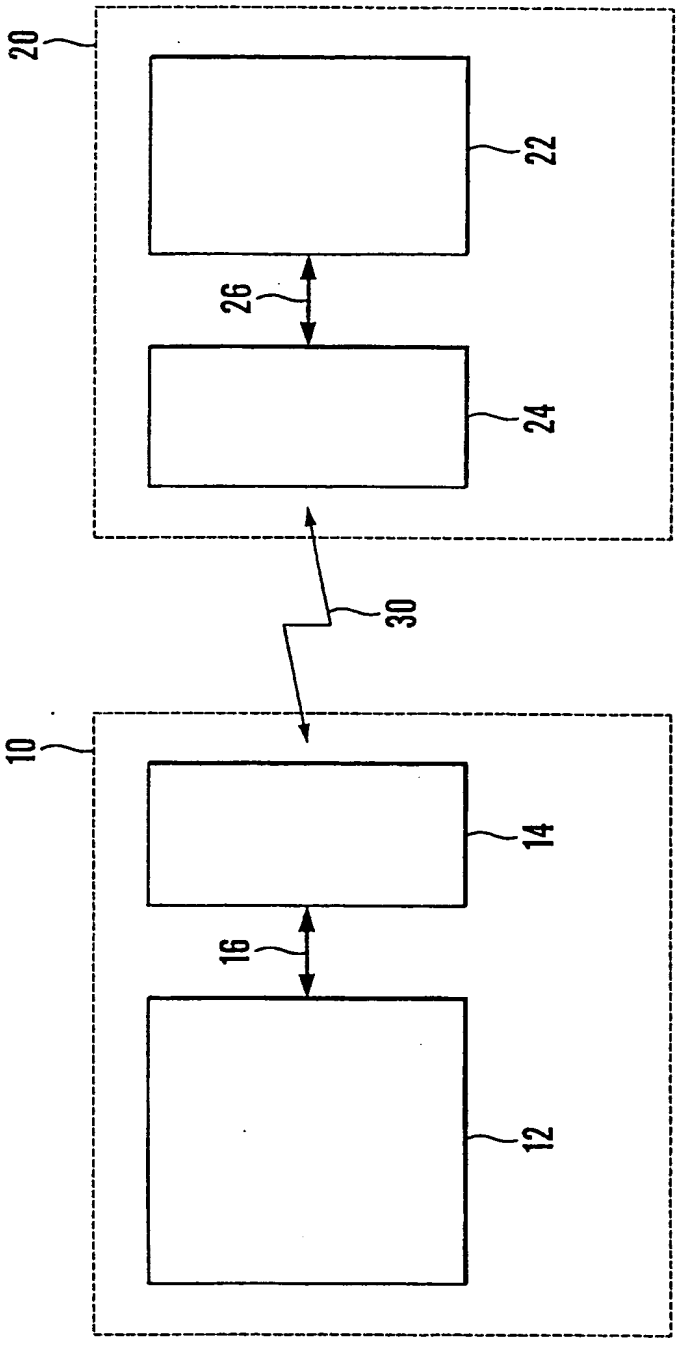


Fig. 1

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 99/00079

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 204 971 A (GEN ELECTRIC CO PLC) 23 November 1988 see the whole document	1-3,5
Y		4,6
Y	WO 93 09621 A (LEE KWANG SIL) 13 May 1993 see abstract; figures 1,2D see page 7, line 22 - page 8, line 29	4,6
A		5
A	GB 2 181 582 A (BLACKWELL VICTOR CAMPBELL) 23 April 1987	
A	WO 96 34333 A (INTERVAL RESEARCH CORP) 31 October 1996	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 April 1999	04/05/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 99/00079

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2204971 A	23-11-1988	NONE	
WO 9309621 A	13-05-1993	KR 9705637 B	18-04-1997
		AT 153202 T	15-05-1997
		AU 658459 B	13-04-1995
		AU 2896992 A	07-06-1993
		BR 9205419 A	19-04-1994
		CA 2098594 A	01-05-1993
		DE 69219756 D	19-06-1997
		DE 69219756 T	18-12-1997
		EP 0565685 A	20-10-1993
		HU 65528 A	28-06-1994
		JP 6511097 T	08-12-1994
		US 5475377 A	12-12-1995
		US 5565857 A	15-10-1996
		CN 1086284 A	04-05-1994
GB 2181582 A	23-04-1987	AU 6476786 A	05-05-1987
		EP 0241504 A	21-10-1987
		WO 8702491 A	23-04-1987
WO 9634333 A	31-10-1996	US 5832296 A	03-11-1998
		AU 5027996 A	18-11-1996
		EP 0823082 A	11-02-1998